Toward Engineering of Security of Information Systems: The Security Acts

Wilson Goudalo
ABE Research
Advanced Business Engineering – ABE
Paris, France
wilson.goudalo@laposte.net

Abstract: **Business professionals and researchers have made considerable efforts and significant technical breakthroughs in information security in the last decades. Nevertheless, companies and organizations continue to incur losses associated with security issues. In order to remedy to this situation, we propose a new approach to information security engineering for companies and organizations. First, this approach is based on the standards and good practices of security, second, is inspired from the best practices and feedback of advances in the engineering of enterprise information systems security, and third, its design takes advantage of more than twelve years of experience in system architecture and information security for reknown banks and financial institutions.**

Our approach to engineering of information systems security aims at:

- reducing losses relating to security issues in companies and organizations, operating on an enhanced and sustained information security;

- improving the reliability of processes in companies and organizations, and assisting companies in legal and regulatory compliance efforts, operating on security indicators and checkpoints at various levels of management;

- helping companies gain competitive advantages through their security management solutions, operating on a global security monitoring system with feedback.

As further development of the basic principle of Security know-how Encapsulation into UML profiles [14], we have introduced the mapping global picture of the Process of Security engineering into the formalism of Business Processes. The purpose of this paper is to provide a clear methodology based on the elaboration of the key Security Acts of the process of information systems security engineering. The paper consists of three major parts:

- Part One recalls the reasons why BPM has been chosen for our process of system information security.

- Part Two develops the key security acts of the process of information systems security engineering.

- Part Three shows some security metrics to illustrate the aims of our works.

Keywords: security acts; security engineering; BPM; enterprise information system security.

I. INTRODUCTION

Business professionals and researchers have made considerable efforts and significant technical breakthroughs in information security [1] - [7]. Nevertheless, companies and organizations continue to incur losses due to security issues [8] – [11]. Taking this unsatisfying situation into account, we have developed a new approach to information security engineering for companies and organizations. Our works aim at bringing a methodological and organizational approach to bond all the stakeholders of a company around the security issue. We use a federator approach based on Business Process Management and provide a real bridge between the enterprise top management level and the daily technical operations level.

Nowadays, business is incorporated in technology. Business security depends on technology security on the one hand side and, on the other hand side, technology security improves business. To achieve an efficient enterprise security, we propose a joint-work of the different teams of a company: the management, business, functional and technical teams [12]. Our approach is reinforced by the McKinsey strategy [13]: *"When business and IT executives jointly take an end-to-end look at business processes, the resulting investments can have up to ten times the impact (to the business) of traditional IT cost reduction efforts"*.

In our recent articles, we showed the encapsulation of Security know-how into UML profiles [14] and introduced the global view on mapping the Process of security engineering into the formalism of Business Processes [15]. The purpose of this paper is to give detailed information on the key security acts of the process of information systems security engineering.

II. BPM NOTIONS AND SECURITY CONCEPTS

Business Process Management is activity undertaken by businesses to identify, evaluate, and improve business processes. A business process is a set of activities organized in a network and performed sequentially or in parallel that combine and implement

 ISBN: 978-1-61208-010-9

multiple resources, capabilities and skills to produce a valuable result or output.

The business process is the most important asset of a company [16]. It is the first step of an enterprise strategy, coming before the other business functions like the functional, the applicative and the technical or technological views [17]. All enterprise architecture methodologies deal with this paradigm: the Praxeme approach [18] relates to the pragmatic and semantic aspects, the Togaf approach [19] to business architecture (Architecture Development Methodology) and business scenario; the USI approach ([20] and [21]) relates to the business view and the Zachman approach ([22], [23] and [24]) relates to the cells « Function/Scope» and « Function/Enterprise Model ». All the other points of view (levels, layers, aspects) of the information system will gradually be developed from the process point of view ([25], [26], [18] and [27]) regardless to the methodology adopted by the company (Top-Down approach) in order to come down to a concrete implementation of the security measures.

Our approach to security engineering covers the security of information systems at each level of their life cycle, by working on four security concepts simultaneously in an attempt of an on-going enhancement. These are the assets and related risks and the security solutions and monitoring indicators.

The security concept of assets describes the main company assets to protect and their value in terms of security. A company or organization asset would then be described as the set of all its properties having value which are necessary to reach its business objectives. It could be information, services provided to clients or partners, transformation processes, know-how and skills inherent to the activity of the company and having value with respect to the stakes of the company. An IS asset is an IS component which supports one or many company assets; therefore the company assets security requires the security of the IS assets supporting them.

The security concept of risks is linked to the security needs of the company assets. Security needs are expressed through three basic criteria: confidentiality, integrity and availability. Security risk depends on the exposure of company assets to risks, the probability of occurrence of a security-relevant event and the actual resulting damage to the assets. The different components of security risk are: the risk itself, the risk factor, the risk impact, threat and vulnerability.

The security solution defines the measures taken to protect company assets against risks, to which they are exposed. When elaborating a security solution, the decision about how an identified risk must be processed, would be to avoid, reduce, transfer or retain that risk.

A solution in itself is a function of the factors listed hereafter: the security policy in force, the asset quotation, the results of the analysis of the identified risk, the nature of the solution and how the latter is designed, implemented, run and managed.

The security concept of monitoring indicators is defined through security quality, in order to reach harmonized monitoring of security efficiency. Quality is evaluated on the basis of all the functional and non-functional requirements [28]. It is an abstract concept whose meaning would be different from one stakeholder to the other (e.g. clients, partners, users, managers, designers, developers and operators). It refers to different concepts depending on the qualified object. To define the security quality requirements concretely, we divided the main concept into some kinds of conceptual quality model [15].

III. SECURITY ACTS OF INFORMATION SYSTEMS

Information systems security engineering is defined as a process that aims at providing global security to enterprise information systems in their eco-system, in order to meet the company stakes. We present below the new design of the global picture of the information security engineering process.

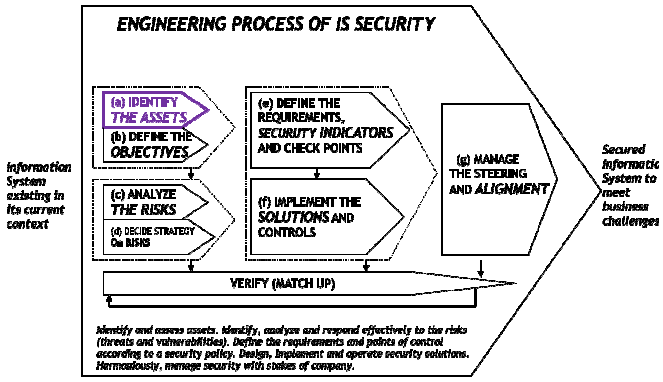

Figure 1. Process of ESIS – the security acts

The security acts of our security engineering process are:

- (a) Identify the company assets.
- (b) Define the security objectives to be met.
- (c) Analyze the security risks.
- (d) Decide strategy on security risks.
- (e) Define the security requirements to cover the risks.
- (f) Select, implement security solutions and verify control tools.
- (g) Manage security and its alignment to companies' objectives.

 ISBN: 978-1-61208-010-9

After the security solutions have been defined, new security risks may occur. The latter might render some security solutions obsolete or might be ignored by the security solutions already implemented. The process of information systems security engineering must be iterative and cyclic to achieve an on-going enhancement. This guarantees the efficient fulfillment of the primary goals of companies' security at any time. For this purpose, we added a transversal security act to insure the auto-adaptation of the process; this is called "Matching". This security act does not exist on its own; it goes together with the security act "Management of security and its alignment with the company objectives" (g).

We split up each security act into a set of security activities and present it according to the business sub-processes formalism.

A. *Identify the company assets*

"Identify assets of companies" is one of the seven security acts of our process of information systems security engineering. In this security act, we include the following security activities:

- List the major assets (such as hardware, software, human, documentary, physical and intangible).
- Specify the use case contexts and the corresponding responsible person (the person who has deep knowledge of its use, its value, and the consequences of compromise) for each asset.
- Define the values held by those assets and their sensitivity to business enterprise, regulation and legislation
  Classify assets and define their quotation, in relation with given security criteria.

We illustrate below the security act "Identify the assets of company", as a sub-process.

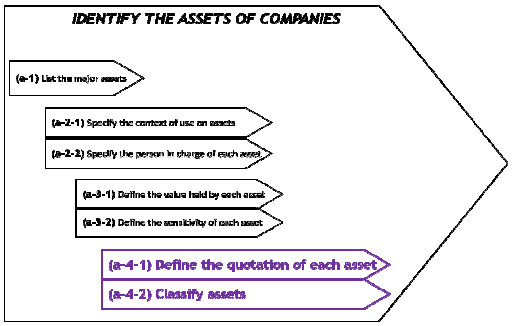

Figure 2. Process of ESIS – the security activities as sub-processes

We recall the characteristics of information system security defined by the three invariant criteria below.

- Confidentiality: Information should not be, made accessible, or disclosed to a user, to an entity or to a system process that is not allowed.
- Integrity: Information should not be amended, altered or destroyed in an unauthorized manner.
- Availability: Access, by an authorized entity, authorized user or authorized process, to services provided by the system, must be always possible. Operations that occupy processing time illegally or that attempt to reach such goal, must be detected and eliminated in time.

Other properties of the information security, such as Proof, Traceability and Authenticity are derived from these three invariants criteria.

The security criteria characterize the constraints on the properties of business assets, describing their security needs. The stakes of companies may be human, financial, branding, regulatory or legal.

We illustrate below the process of quotation those results in secure assets classification.

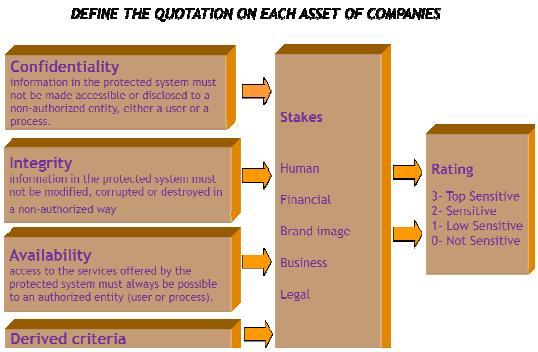

Figure 3. Process of ESIS – the quotation of assets

B. *Classify the company assets*

It's not possible to secure every asset of a company against every imaginable risk. Thus, we must classify assets on which we operate, in order to efficiently protect the intellectual property, protect confidential information from unauthorized use or disclosure and facilitate SLA (Service Level Agreements) and business continuity management. Security classification of assets becomes necessary to provide and improve business activities.

Security classification of assets meets both business and operational needs. It is based on the real value of the assets for companies in terms of business, brand image, human resources, and financial, legal and regular aspects. Actually, we dissociate the security classification of assets from the activities related to threat and risk analysis. In our process of information system security engineering, the security activity "security classification of assets" is an element of security act "Identify assets". The results of the three

 ISBN: 978-1-61208-010-9

security acts “Identify assets” “Define the objectives of security” and “Analyze the risks” are used in the security act “Decide strategy on risks”.

We illustrate below the main steps of the security activity “Secure classification of assets”, as a sub-process.

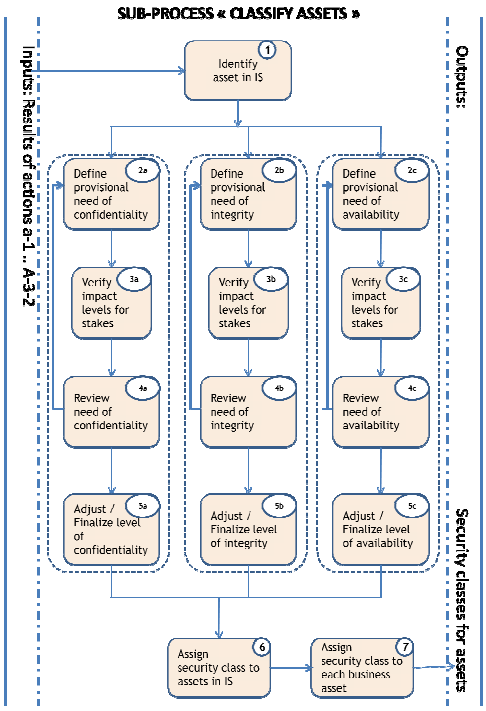

Figure 4. Process of ESIS – the sub-processes of security classification of assets

The security classification of assets

- Operates on three main security criteria (Confidentiality, Integrity, Availability) and derived criteria;
- Takes into account companies stakes (from strategic management);
- Provides four sensitivity classes (non sensitive, low sensitive, sensitive and top sensitive).

We descript the sub-process “classify assets of company” in seven steps, and we elaborate the input and output of each step.

Step-1: Identify asset in the Information System of company. For each asset defined in asset list (business asset or essential asset to support the business), we identify the related IS assets, according to conceptual model of company assets [15], and we specify (verify) the owner of each asset.

Step-2: Define provisional level, about need of security criteria Define security needs for the related IS asset, in terms of confidentiality (a), integrity (b) and availability (c), according to the real (intrinsic) value of each asset.

Step-3: Verify the impact levels for stakes of company. Verify the impact levels for stakes of company, in terms of human, financial, brand image, business and legal, according to the organization, environment and mission of a company.

Step-4: Review provisional level, about need of security criteria. Review the appropriateness of the provisional need of security criteria (confidentiality, integrity and availability), according the level of impacts assessment on stakes of company.

Step-5: Adjust/Finalize level, about need of security criteria. Adjust/Finalize need of security criteria (confidentiality, integrity and availability) to each asset in IS, according to security strategy of the company, the real environmental context of the company, and the security policy in force in the company.

Step-6: Assign security class to assets in IS. Assign the resulting security classes to main assets in IS, and determine the classification.

Step-7: Assign security class to each business asset. Assign the resulting security class to main business assets according the classification determined in step-6, and document the classification in a language understandable by the business.

We recall that security engineering is assumed through ongoing process, like Deming wheel [14]. So it is necessary to maintain classification and conduct continuous review.

We synthesize the provided four classes of sensitivity, in the table below.

TABLE 1. SECURITY CLASSIFICATION OF ASSETS

Security classes	Description	Examples of assets *(*)*
Class-0: Not sensitive	Assets that enter in the normal course of business or support of business, and that don't present any stake for a company in case of loss of confidentiality, integrity, availability, or derived criteria.	Provided courses, planning of courses, dates of exams, professional information on organizers.

 ISBN: 978-1-61208-010-9

Security classes	Description	Examples of assets *(*)*
Class-1: Low sensitive	Assets that enter in the normal course of business or support of business, and that present low stake (low levels of financial loss) for a company in case of loss of confidentiality, integrity, availability, or derived criteria.	Professional information on students, detailed course material, earnings per course.
Class-2: Sensitive	Assets that enter in the normal course of business or support of business, and that present serious stake (important level of financial loss, loss of competitive advantage, loss of confidence in business strategy, damage to partnerships, relationships and reputation) for a company in case of loss of confidentiality, integrity, availability, or derived criteria.	User access of students, examination subjects, enlistment strategy of students.
Class-3: Top sensitive	Assets that enter in the normal course of business or support of business, and that present vital stake (extreme damage to the integrity, effective service delivery, loss of life, substantial financial loss, major economic impact) for a company in case of loss of confidentiality, integrity, availability, or derived criteria.	User access of organizers, personal medical record of students, online exam service.

(*) – In order to comply with the confidentiality clause of our business agreements with customers, we have used a fictive e-Learning company as basis to build all the examples presented here.

We elaborate the security classification of assets according to their value and importance for the target companies. We assign to a handled group of assets, at least the highest security class level of all assets forming the (no dissociable) group. In the case of some combination of assets, the real security class of the resulting combination must be determined. The security classification of an asset is adjustable depending on its life cycle and on its participation in the business cycles in a company.

For each security class we develop a set of procedures for storage, copying, access, transmission, communication, disclosure, destruction and accountability.

C. Define the security objectives to be met

In defining the security objectives, we must,

- Express the security needs on the assets, for the first time.
- Establish the specifications appropriate to the triptych: “identified security needs”, “analyzed security risks” and “security policy of the company”.

D. Analyze the security risks

In this security act, we mention the following activities:

- Identify the inherent vulnerabilities of each asset that expose it to potential threats
- Identify threats to which each asset is exposed
- Estimate the probability of occurrence of each threat (ignoring the context and the environment).
- Analyze the impact of the occurrence of each threat.
- Estimate the likelihood of occurrence of each threat (taking into account the facts, the existing measures, and environment).
- Define the probability of occurrence, depending on the context.
- Assess the overall level to which each asset is exposed, taking into account all evidence obtained above.

There are different methods of risk analysis. We have developed the key security activities that are in use in the industries.

E. Decide strategy on security risks

In order to make a decision about the treatment of security risks, we must, for the first time, decide which type of treatment to apply for each identified risk. The decision of treatment belongs to one of these four types: acceptance, avoidance, reduction, transfer.

After a strategy has been adopted, we deduce the residual risks.

If the inferred residual risks are *not acceptable, we make another decision about the type* of risk treatment. In the general case, the act of deciding which treatment of risk to adopt leads to the reasonable decision of

 ISBN: 978-1-61208-010-9

reducing the risk. This results in the definition of the security requirements, to mitigate each risk.

F. Define the security requirements to cover the risks

The security requirements lead to define the type of controls: Correction, Detection, Deterrence and / or Prevention. We insist on the consistency of security requirements with the security objectives and with the treatment strategy. We recall that the security objectives are themselves consistent with the risks, needs and security policy.

The security requirements cover all security objectives and define two types of requirements: functional requirements (security features to provide) and the associated insurance requirements (evidence on the quality of features).

G. Select, implement and verify control tools

In this security act, we first choose the security measures to meet the security requirements. On the next step, those measures are implemented, tested, integrated deployed.

Security measures can be physical, organizational and / or software. They are kind of products from suppliers or specific developments.

In all cases, this security act is the sound basis on which the IS security stands. Most approaches to security and security research are limited to this security act.

H. Manage of security and its alignment to company objectives

In this security act, we mention the following activities:

- Develop a document of the security policy in accordance with the corporate objectives, in its ecosystem competitive, regulatory and legal.
- Decline of the security policy features in security and safety indicators qualify, quantifiable and verifiable.
- Review regularly (at intervals of time defined) the security policy and occasionally (not compulsory and optional) in case of significant events.
- Ensure the harmony between the different activities of security (from “a” to “g”) and make them comply with the security policy.

IV. ILLUSTRATION - SECURITY METRICS

In a Top-Down approach (from strategic management level to technical daily operations level), applying the methodology in place in the company to the process of Information System Security Engineering will lead to the concrete implementation of security solutions. We suggest below an architectural diagram which illustrates the concrete implementation of security solutions and the control points providing security metrics.

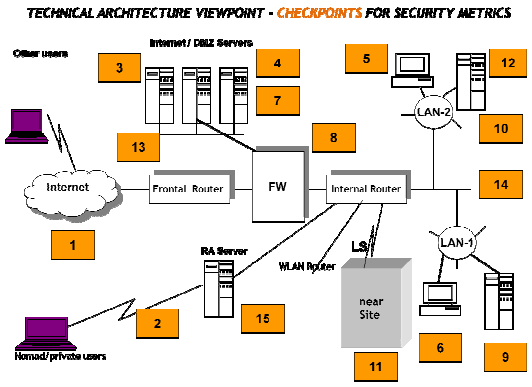

Figure 5. Process of ESIS – the technical implementation diagram

Security metrics are necessary to manage strategic alignment. The top management is interested in:

1. Corporate Reports as money, ratios, index
2. Measures of broad matters as quality compare to that of competitors; time required to launch new products
3. Measures that help to establish departmental quality goals and to evaluate departmental performance against goals.
4. Technological units of measure for individual elements of product, process, service

The main objective is “Moving up the stack without losing clarity”. Our approach of Engineering of Information Security applied with Enterprise Architecture framework in place provides the real solution.

V. CONCLUSION

To stay under the admissible size of this article, we will develop the other security activities related the seven security acts (from “a” to “g”) in future works,.

In this paper we have presented the security activities related to assets classification in more details. The preference of security activity “Classify assets” is motivated by the nowadays period to which companies are facing.

After the era of the extended enterprise where the information system was opened to customers and partners, we are witnessing two phenomena, simultaneously: “the consumerism of computing” and “the cloud computing”. With "the consumerism of computing" era, we observe the import innovative uses from home to work, the blurring the boundary between

 ISBN: 978-1-61208-010-9

home and work, the mutual influence between technology and uses. With “the Cloud Computing”, PAAS, IAAS, SAAS, and others, the IS assets of enterprise are no more storage in well known geographic place. In these contexts the perimeter based security is obsolete. The challenge is in assisting. The CSO has to get closer to the core business of a company. While having an adaptive communication to the management and to all levels of the company, he also has to understand the strategy, and the technical applications.

The CSO classifies the information of the companies and their assets. So in this context, access to information assets is defined according to:

- Who is the person.
- The trust level of the terminal.
- Where is the terminal located.

The access level to asset depends on the classification of asset and the trust level of these three parameters.

VI. REFERENCES

[1] David Elliott Bell and Leonard J. LaPadula. “Secure Computer Systems : Unified Exposition and Multics Interpretation”. Technical Report ESD-TR-75-306, MTR-2997, MITRE, Bedford, Mass, 1975.

[2] Morrie Gasser. “Building a secure computer system”, Van Hoostrand and Reinhold ed., 1988.

[3] Charles Bennett. “Quantum Cryptography – Uncertainty in the Service of Privacy”. Science Vol. 257. no. 5071, pp. 752 - 753. August 1992.

[4] Frédéric Cuppens. “A Logical Analysis of Authorized and Prohibited Information Flows”. IEEE Symposium on Security and Privacy. Oakland, 1993.

[5] Richard J. Hughes, Jane E. Nordholt, Derek Derkacs and Charles G. Peterson. “Practical free-space quantum key distribution over 10 km in daylight and night”. New journal of physics 4 (2002). http://www.iop.org/EJ/abstract/1367-2630/4/1/343/

[6] William Stallings. “Cryptography and Network Security – Principles and practice”. Fourth edition. ISBN 978-0-1318-7316-2. Prentice Hall Editions. New Jersey - USA 2006.

[7] SANS (SystAdmin, Audit, Network, Security), “Rapport 2009 CWE/SANS des 25 erreurs de programmation les plus dangereuses”, SANS 2009. http://www.sans.org/top25errors/ Last access date : may 2011.

[8] Security for Business Innovation Council; “The Time is now: making information security strategic to business innovation”; RSA Security; Bedford MA. 2008.

[9] Benoît Dupont et Bénoît Gagnon. “La sécurité précaire des données personnelles en Amérique du Nord", Note de recherche n°1, Chair de recherche du Canada en sécurité, identité et technologie, 2008.

[10] http://www.cnis-mag.com Site de magasine sur les problématiques de l’informatique et de la sécurité. Last access date : may 2011.

[11] Jeremy Epstein, "Security Lessons Learned from Société Générale", IEEE SECURITY & PRIVACY, Vol. 6, 03, pp. 80-82, MAY/JUNE, 2008.

[12] Goudalo Wilson, “Business Security” in Engineering Secure Complex Software Systems and Services. Proceedings of the European Research Consortium for Informatics and Mathematics Seminar on ICT Security. Brussels, 16 October 2008. http://www.ercim.org/

[13] “Managing IT in a Downturn - Beyond Cost Cutting”. McKinsey on Business Technology. Fall 2008

[14] Goudalo Wilson et Seret Dominique. "Toward the Engineering of Security of Information Systems (ESIS): UML and the IS Confidentiality". Proceedings of the 2008 Second International Conference on Emerging Security Information, Systems and Technologies. Pages 248-256. IEEE Computer Society Washington, DC, USA. ISBN: 978-0-7695-3329-2.

[15] Wilson Goudalo et Dominique Seret. "The Process of Engineering of Security of Information Systems (ESIS): The Formalism of Business Processes ". Securware, pp.105-113, 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 2009.

[16] Marwane El Kharbili, Sebastian Stein, Ivan Markovic and Elke Pulvermüller. “Towards a Framework for Semantic Business Process Compliance Management”. Proceedings of the Workshop SBPM 2007, Innsbruck 2007, ISSN 1613-0073

[17] Ivan Markovic, Alessandro Costa Pereira. “Towards a Formal Framework for Reuse in Business Process Modeling”. In Workshop on Advances in Semantics for Web services (semantics4ws), in conjunction with BPM '07. Brisbane (Australia) 2007.

[18] Praxeme institute – Public methodology of Enterprise Architecture. http://www.praxeme.org. Last access date : may 2011.

[19] TOGAF, The Open Group Architecture cadre. Version 8.1 “Enterprise Edition” 2003.

[20] Longépé Christophe. “The Enterprise Architecture IT Project – the Urbanisation Paradigm”. Penton, 2002

[21] Club Urba SI. "Pratiques de l’Urbanisme des Systèmes d’Information en entreprises". Publibook, 2003.

[22] John Zachman and John Sowa. “Extending and Formalizing the Framework for Information Systems Architecture”. IBM Systems Journal. Volume 31, No. 3, pp 590-616, 1992.

[23] Jaap Schekkerman. “How to Survive in the Jungle of Enterprise Architecture Frameworks”, Trafford, Third edition, 2006

[24] Tony Brown. “The Value of Enterprise Architecture”. ZIFA report, 2005.

[25] Douglas W. McDavid. "A standard for business architecture description" in Enterprise Solutions Structure. IBM Systems Journal, Volume 38, Number 1, 1999

[26] Celia Talma Martins and António Lucas Soares. “Dissecting Inter-Organizational Business Process Modeling: A Linguistic and Conceptual Approach” in Network-Centric Collaboration and Supporting Frameworks. pp 221-228. Springer Boston, 2006. ISBN : 978-0-387-38266-1.

[27] [GAN-08] Eswar Ganesan, Ramesh Paturi. “Bulding Blocks for Enterprise Business Architecture”. Infosys Research Publications. SETILabs Briefings. Volume 6, Number 4, 2008.

[28] Beatriz. Bernardez, Amador Duran, and Marcela Genero. “Metrics for use cases: a Survey of Current Proposals”. In M. Genero, M. Piattini, and C. Colero Editors, Metrics for Software Conceptual Models. Pages 59-98. Imperial College Press, 2005.

 ISBN: 978-1-61208-010-9